WHAT IS CLAIMED IS:

1. An encrypted network system, comprising:

a network to transmit an encrypted packet; and

a computer to receive said encrypted packet from said network, and to perform a decryption operation thereupon to convert said encrypted packet to a decrypted packet, said computer including:

a network interface to provide electronic communication between said computer and said network,

a network driver to regulate said decryption operation,

a controller to perform said decryption operation,

a host memory to store data that is used or generated by said decryption operation, and

a bus providing electronic communication among said network interface, said network driver, said host memory and said controller, said controller asserting an interrupt prior to a complete transfer of said decrypted packet from said controller to said host memory.

2. The encrypted network system of claim 1, wherein at least one security association (SA) is stored in said host memory.

3. The encrypted network system of claim 2, wherein said network driver parses said encrypted packet, matches said encrypted packet with one of said at least one SA and instructs said network interface to transfer said encrypted packet and said one SA across said bus to said controller.

4. The encrypted network system of claim 1, wherein said network interface includes a cryptography accelerator.

5. The encrypted network system of claim 1, wherein said controller transfers said decrypted packet across said bus from said controller to said host memory.

6. The encrypted network system of claim 1, wherein said controller asserts an additional interrupt after completion of said decryption operation.

7. The encrypted network system of claim 1, wherein said network driver specifies an average latency value to said controller for use in said decryption operation.

8. A computing system for performing a decryption operation on an encrypted packet, comprising:

a network driver to regulate said decryption operation;

a controller to perform said decryption operation;

a host memory to store data that is used or generated by said decryption operation; and

a bus providing electronic communication among said network driver, said host memory and said controller, said decryption operation converting said encrypted packed into a decrypted packet, and said controller asserting an interrupt prior to a complete transfer of said decrypted packet from said controller to said host memory.

9. The computing system of claim 8, wherein said computer further includes a network interface to provide electronic communication between said computer and a network.

10. The computing system of claim 9, wherein at least one security association (SA) is stored in said host memory.

11. The encrypted network system of claim 10, wherein said network driver parses said encrypted packet, matches said encrypted packet with one of said at least one SA and instructs said controller to transfer said encrypted packet and said one SA across said bus to said controller.

12. The computing system of claim 8, wherein said network interface includes a cryptography accelerator.

13. The computing system of claim 8, wherein said controller transfers said decrypted packet across said bus from said controller to said host memory.

14. The computing system of claim 8, wherein said controller asserts an additional interrupt after completion of said decryption operation.

15. The computing system of claim 8, wherein said network driver specifies an average latency value to said controller for use in said decryption operation.

16. A method of decrypting an encrypted packet received by a computing system, comprising:

receiving said encrypted packet from a network;

converting said encrypted packet to a decrypted packet;

transferring said decrypted packet to a host memory; and

asserting an interrupt at a time before completing said transfer of said decrypted packet to said host memory.

17. The method of claim 16, wherein prior to converting said encrypted packet, said method further includes:

issuing a decryption command to a controller; and

determining a time for said assertion of said interrupt in response to said decryption command.

18. The method of claim 16, wherein said step of converting said encrypted packet to said decrypted packet further includes:

parsing said encrypted packet;

matching said encrypted packet with a corresponding security association (SA) stored in said host memory; and

transferring said encrypted packet and said corresponding SA to a controller.

19. The method of claim 16, wherein said step of converting said encrypted packet to said decrypted packet further includes authenticating said decrypted packet.

20. The method of claim 16, further including asserting an additional interrupt upon completion of said transfer of said decrypted packet to said host memory.

21. The method of claim 16, further including indicating said decrypted packet to a protocol stack after asserting said interrupt.

22. A program code storage device, comprising:

a machine-readable storage medium; and

machine-readable program code, stored on the machine-readable storage medium, the machine-readable program code having instructions to:

receive said encrypted packet from a network;

convert said encrypted packet to a decrypted packet;

transfer said decrypted packet to a host memory; and

assert an interrupt at a time before completing said transfer of said decrypted packet to said host memory.

23. The system of claim 22, wherein prior to the instructions to convert said encrypted packet, said system further includes instructions to:

issue a decryption command to a controller; and

determine a time for said assertion of said interrupt in response to said decryption command.

24. The system of claim 22, wherein said instructions to convert said encrypted packet to said decrypted packet further includes instructions to:

parse said encrypted packet;

match said encrypted packet with a corresponding security association (SA) stored in said host memory; and

transfer said encrypted packet and said corresponding SA to a controller.

25. The method of claim 22, wherein said instructions to convert said encrypted packet to said decrypted packet further includes instructions to authenticate said decrypted packet.

26. The system of claim 22, further including instructions to assert an additional interrupt upon completion of said transfer of said decrypted packet to said host memory.

27. The method of claim 22, further including instructions to indicate said decrypted packet to a protocol stack after the instruction to assert said interrupt